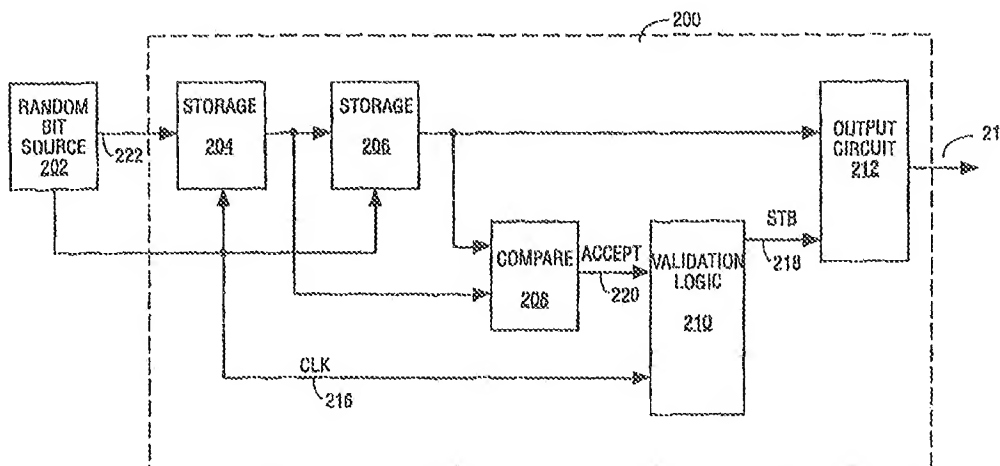




INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification ⁷ : H04L 9/00		A2	(11) International Publication Number: WO 00/59153
			(43) International Publication Date: 5 October 2000 (05.10.00)
(21) International Application Number: PCT/US00/06916		(81) Designated States: AE, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CR, CU, CZ, DE, DK, DM, DZ, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, US, UZ, VN, YU, ZA, ZW, ARIPO patent (GH, GM, KE, LS, MW, SD, SL, SZ, TZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).	
(22) International Filing Date: 16 March 2000 (16.03.00)			
(30) Priority Data: 09/283,096 31 March 1999 (31.03.99) US			
(71) Applicant (for all designated States except US): INTEL CORPORATION [US/US]; 2200 Mission College Boulevard, Santa Clara, CA 95052 (US).			
(72) Inventors; and			
(75) Inventors/Applicants (for US only): WELLS, Steven, E. [US/US]; 4236 Weathervane Court, El Dorado Hills, CA 95762 (US); WARD, David, A. [US/US]; 2808 Honeysuckle Way, Sacramento, CA 95826 (US).		Published Without international search report and to be republished upon receipt of that report.	
(74) Agents: MILLIKEN, Darren, J. et al.; Blakely, Sokoloff, Taylor & Zafman LLP, 7th floor, 12400 Wilshire Boulevard, Los Angeles, CA 90025 (US).			

(54) Title: DUTY CYCLE CORRECTOR FOR A RANDOM NUMBER GENERATOR



(57) Abstract

A method and apparatus for producing a corrected bit stream from a random bit stream output by a random bit source. Sequential pairs of bits in the random bit stream are compared. If both bits in a pair of bits are identical, the output bits are discarded. If both bits in a pair of bits are different, one bit of the pair of bits is taken as the output bit.

(19) 日本国特許庁 (J P)

(12) 公表特許公報 (A)

(11) 特許出願公表番号

特表2002-540482

(P2002-540482A)

(43) 公表日 平成14年11月26日 (2002. 11. 26)

(51) Int.Cl. ⁷	識別記号	F I	テーマト* (参考)
G 0 9 C 1/00	6 5 0	G 0 9 C 1/00	6 5 0 B 5 J 1 0 4
G 0 6 F 7/58		G 0 6 F 7/58	A

審査請求 未請求 予備審査請求 有 (全 43 頁)

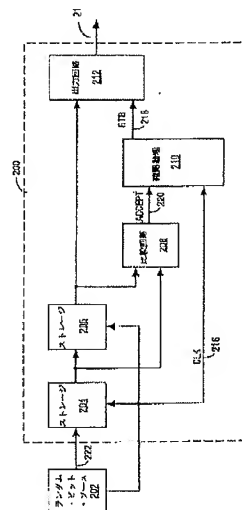
(21) 出願番号 特願2000-608542(P2000-608542)
(86) (22) 出願日 平成12年3月16日 (2000. 3. 16)
(85) 翻訳文提出日 平成13年9月28日 (2001. 9. 28)
(86) 国際出願番号 P C T / U S 0 0 / 0 6 9 1 6
(87) 国際公開番号 W O 0 0 / 5 9 1 5 3
(87) 国際公開日 平成12年10月5日 (2000. 10. 5)
(31) 優先権主張番号 0 9 / 2 8 3 , 0 9 6
(32) 優先日 平成11年3月31日 (1999. 3. 31)
(33) 優先権主張国 米国 (U S)

(71) 出願人 インテル・コーポレーション
アメリカ合衆国 95052 カリフォルニア
州・サンタクララ・ミッション カレッジ
ブーレバード・2200
(72) 発明者 ウエルズ・スティーブン・イー
アメリカ合衆国・95762・カリフォルニア
州・エル ドラド ヒルズ・ウェザーペイ
ン コート・4236
(72) 発明者 ワード, デイビッド・エイ
アメリカ合衆国・95826・カリフォルニア
州・サクラメント・ハニーサックル ウェ
イ・2808
(74) 代理人 弁理士 山川 政樹
Fターム(参考) 5J104 FA00

(54) 【発明の名称】 乱数発生器用デューティ・サイクル修正器

(57) 【要約】

ランダム・ビット・ソースによって出力されたランダム・ビット・ストリームから、修正後のビット・ストリームを生成する方法および装置。それにおいては、ランダム・ビット・ストリーム内のビットの連続するペアが比較される。ビットのペアを構成する2つのビットがまったく等しい場合には、出力されたビットが破棄される。ビットのペアを構成する2つのビットが互いに異なる場合には、そのビットのペアの一方のビットを出力ビットとして採用する。



【特許請求の範囲】

【請求項1】 ランダム・ビット・ソースによって出力されたランダム・ビット・ストリームから修正後のビット・ストリームを生成する方法において：

前記ランダム・ビット・ストリーム内のペアとなるビットを互いに比較するステップ；

前記ビットが等しい場合には前記ペアとなるビットを破棄するステップ；

前記ランダム・ビット・ストリーム内のもう1つのビットを破棄するステップ；および、

前記ペアとなるビットが等しくない場合には前記ペアとなるビットのうちの1つを出力するステップ；

を包含することを特徴とする方法。

【請求項2】 前記もう1つのビットを破棄するステップは、前記比較するステップに先行して起こることを特徴とする前記請求項1記載の方法。

【請求項3】 前記もう1つのビットを破棄するステップは、前記ペアとなるビットを破棄するステップに後続して起こることを特徴とする前記請求項2記載の方法。

【請求項4】 前記ペアとなるビットのうちの1つを出力するステップは、前記ペアとなるビットのうちの最初のビットを出力するステップを構成することを特徴とする前記請求項1記載の方法。

【請求項5】 前記ペアとなるビットのうちの1つを出力するステップは、前記ペアとなるビットのうちの2番目のビットを出力するステップを構成することを特徴とする前記請求項1記載の方法。

【請求項6】 さらに、直列結合されたラッチのペア内に前記ペアとなるビットを同期させてラッチするステップを含むことを特徴とする前記請求項1記載の方法。

【請求項7】 さらに：

その後続く別のペアとなるビットを比較するステップ；および、

前記ビットを比較した2つのペアの間ある、前記ランダム・ビット・ストリーム内のビットを破棄するステップ；

を包含することを特徴とする前記請求項 1 記載の方法。

【請求項 8】 さらに、前記ペアとなるビットが等しいか等しくないかによらず、前記ランダム・ビット・ストリーム内の前記もう 1 つのビットを破棄するステップを含むことを特徴とする前記請求項 1 記載の方法。

【請求項 9】 ランダム・ビット・ソースから一様なデューティ・サイクルの出力を生成する前記方法は、ネットワーク内の複数のコンピュータ間における安全な通信のための暗号システムに使用されるランダムなバイナリ数を生成するように動作し得る乱数発生器に使用されることを特徴とする前記請求項 2 記載の方法。

【請求項 10】 ランダム・ビット・ソースによって出力されたランダム・ビット・ストリームから修正後のビット・ストリームを生成するためのデューティ・サイクル修正器回路において：

入力および出力を有し、前記入力が前記ランダム・ビット・ソースからランダム・ビット・ストリームを受け取るべく結合された第 1 のストレージ回路；

入力および出力を有し、前記入力が前記第 1 のストレージ回路の出力に結合された第 2 のストレージ回路；

前記第 1 のストレージ回路の出力および前記第 2 のストレージ回路の出力に結合された比較回路；および、

前記比較回路の出力を受け取る第 1 の入力、および周期的な信号を受け取る第 2 の入力を有する確認論理であって、前記第 1 のストレージ回路または前記第 2 のストレージ回路内にストアされたデータが、修正後のビット・ストリーム内のビットであるとき、それを示す信号を出力する確認論理；

を備えることを特徴とするデューティ・サイクル修正器回路。

【請求項 11】 前記第 1 のストレージ回路および前記第 2 のストレージ回路は、ラッチを包含することを特徴とする前記請求項 10 記載のデューティ・サイクル修正器回路。

【請求項 12】 前記比較回路は、エクスクルーシブオア・ゲートを包含することを特徴とする前記請求項 10 記載のデューティ・サイクル修正器回路。

【請求項 13】 さらに、前記確認論理によって出力された前記信号を受け

取るべく結合され、かつ前記第 1 または第 2 のストレージ回路にストアされたビットを受け取るべく結合された出力回路であって、前記ビット・ストリーム内の修正後のビットを出力する出力回路を備えることを特徴とする前記請求項 10 記載のデューティ・サイクル修正器回路。

【請求項 14】 前記出力回路はストレージ回路を包含することを特徴とする前記請求項 13 記載のデューティ・サイクル修正器回路。

【請求項 15】 前記確認論理は：

前記ランダム・ビット・ソースのクロック出力に結合されたトランスペアレント・ラッチ；および、

前記トランスペアレント・ラッチの出力に結合された第 1 の入力、および前記比較回路の出力に結合された第 2 の入力を有するアンド・ゲート；

を包含することを特徴とする前記請求項 10 記載のデューティ・サイクル修正器回路。

【請求項 16】 前記確認論理は：

前記ランダム・ビット・ソースのクロック出力に結合されたモジュロ X カウンタであって、X は 1 より大きい整数とするモジュロ X カウンタ；および、

前記モジュロ X カウンタの出力に結合された第 1 の入力、および前記比較回路の出力に結合された第 2 の入力を有するアンド・ゲート；

を包含することを特徴とする前記請求項 10 記載のデューティ・サイクル修正器回路。

【請求項 17】 コンピュータとネットワーク・メディアの間においてメッセージの送信および受信を行うべく動作し得るネットワーク・インターフェース・デバイス；および、

前記コンピュータから送信されるメッセージの符号化および復号化を行うべく動作し得る暗号化回路／解読回路であって、ランダム・ビット・ストリームを生成するように動作し得る乱数発生器を有し、それにおいて前記乱数発生器は：

未修正ビット・ストリームを出力するように動作し得る乱数発生器；および、
デューティ・サイクル修正器回路であって：

入力および出力を有し、前記入力が前記ランダム・ビット・ソースから前記未

修正ランダム・ビット・ストリームを受け取るべく結合された第１のストレージ回路；

入力および出力を有し、前記入力の前記第１のストレージ回路の出力に結合された第２のストレージ回路；

前記第１のストレージ回路の出力および前記第２のストレージ回路の出力に結合された比較回路；および、

前記比較回路の出力を受け取る第１の入力、および周期的な信号を受け取る第２の入力を有する確認論理であって、前記第１のストレージ回路または前記第２のストレージ回路内にストアされたデータが、修正後のビット・ストリーム内のビットであるとき、それを示す信号を出力する確認論理；

を包含するデューティ・サイクル修正器回路；

を備えるものとする暗号化回路／解読回路；

を備えることを特徴とするコンピュータ。

【請求項１８】 前記暗号化回路／解読回路は、さらに暗号ベースの暗号化方法を使用する前記コンピュータによって送信され、受信されるメッセージの符号化および復号化を行うべく動作し得ることを特徴とする前記請求項１７記載のコンピュータ。

【請求項１９】 前記暗号ベースの暗号化方法は、単一キーシステムであることを特徴とする前記請求項１９記載のコンピュータ。

【請求項２０】 前記暗号ベースの暗号化方法は、公開キー／秘密キーシステムであることを特徴とする前記請求項１９記載のコンピュータ。

【発明の詳細な説明】

【０００１】

(技術分野)

本発明は、全体的にコンピュータ・セキュリティに関し、より詳細に述べれば、乱数発生器におけるほぼ一様なデューティ・サイクルの発生に関する。

【０００２】

(発明の背景)

乱数発生回路は、各種の電子応用において使用されている。乱数発生器に関する重要な応用の１つに、メッセージ・データの暗号化と解読が行なわれるコンピュータ・セキュリティの分野におけるものがある。暗号システムは、データを、符号化したメッセージに変える変換を含み、それが送信されたとき、意図された受取人だけがそれを復号することができる。もっとも一般的な暗号テクニックにおいては、暗号（キー）が使用され、送り側はそれを用いてメッセージを符号化し、受け側はそれを用いて当該符号化されたメッセージを復号する。広く知られた暗号システムには、メッセージの符号化および復号化に単一のキーを使用する方法と、メッセージの符号化とその復号化にそれぞれ別のキーを使用する方法がある。

【０００３】

メッセージの符号化および復号化に使用されるキーは、基本的にバイナリ・データ・パターンであり、それに照らしてメッセージの処理、すなわちフィルタリングが行なわれる。効果的な暗号システムは、十分に大きなビット数を有し、再生がほとんど不可能なキーの使用を必要とする。さらに、キーを構成するデータ・パターンは、そのキーによって符号化が行なわれたメッセージ内において、それらのパターンないしはパターン群を予測不能にできる十分なランダム性を有していなければならない。したがって効果的な暗号システムには、メッセージ内のバイナリ・データが完全に予測不能な態様で変換されることを保証するように、質の高い乱数発生器を使用する必要がある。一般に、暗号スキームにおけるランダム性の欠如は、符号化済みデータと未符号化データの間に、ある種の相関をもたらす。その後、この相関を使用し、符号化済みメッセージに基づいて試行錯誤

を繰り返し、可能性のある出力パターンの予測といったテクニックを通じて、コードの盗み出しが可能になる。

【0004】

バイナリ乱数に望ましい特徴は、純粋にランダムな順序において「0」と「1」のビットが出力されることである。すなわち、あらゆる時点において出力ビットの値が完全に予測不能となることである。乱数発生器の出力のデューティ・サイクルは、無限の標本サイズにわたって約50パーセントとなり、出力が論理ロー（「0」）になる確率と、出力が論理ハイ（「1」）になる確率が等しくなることが望ましい。また、乱数発生器によって示される任意ビットと他のビットの間の相関が低く（たとえば、約ゼロの相関）、出力ビットの間のフーリエ分布が平坦になることが望ましい。

【0005】

しかしながら、現在知られている乱数発生器は、統計的に有意な標本サイズにわたって「0」の数と「1」の数が等しくない傾向にある。従来技術の乱数発生器が様でないデューティ・サイクルとなる共通の理由としては、禁止されたセットアップ／ホールドタイムの間にデータがラッチされたとき、一般に、乱数発生器を構成するラッチが2つの状態のうちの一方に偏ることが挙げられる。乱数発生器におけるデューティ・サイクルの変動を抑える現在の一般的な方法は、ランダム・ビット・ソースの出力段におけるリニア・フィードバック・シフト・レジスタ（LFSR）の使用が関連する。

【0006】

図1は、従来技術における乱数発生器の一例を示しており、ランダム・ビット・ソース102の出力と結合されるリニア・フィードバック・シフト・レジスタ104を使用する。LFSR 104は、多数のラッチ105とゲート106を含み、それを通じてランダム・ビット・ソース102からの出力ビットが伝播される。出力ビットの状態は、ゲート106によってランダムに反転され、ビットの順序がさらに、ラッチ105を通るビットのフィードバックを介して攪乱される。

【0007】

概して、図 1 に示したようなリニア・フィードバック・シフト・レジスタは、特定の不利益を有し、しかも典型的なランダム・ビット・ソースによってもたらされる一様でないデューティ・サイクル特性の完全な修正が得られない。LFSR 104 によって示されるように、通常、LFSR 自体が複数のラッチとゲートを包含している。これらのラッチとゲートは、ランダム・ビット・ソース 102 内のラッチの場合に同じく、特定の状況下において「0」または「1」のラッチへ偏る傾向にある。つまり、通常の LFSR 自体が「1」と「0」の一樣なデューティ・サイクルを生成せず、そのためランダム・ビット・ソースにおけるデューティ・サイクルの変動を完全には修正し得ない。

【0008】

それ以外にもリニア・フィードバック・シフト・レジスタは、多数のラッチとゲートを必要とするという不利益がある。たとえば、図 1 に示したような 32 ビットの LFSR であれば、32 個の D タイプのラッチが必要になるだけでなく、多数の組み合わせゲートが必要になる。このことは、この種の LFSR を使用する乱数発生器のために必要となるシリコン面積を格段に増加させることになる。

【0009】

(発明の要約)

ここでは、ランダム・ビット・ソースによって出力されたランダム・ビット・ストリームから、修正後のビット・ストリームを生成する方法および装置を開示する。それにおいては、ランダム・ビット・ストリーム内のビットの連続するペアが比較される。ビットのペアを構成する 2 つのビットがまったく等しい場合には、出力されたビットが破棄される。ビットのペアを構成する 2 つのビットが互いに異なる場合には、そのビットのペアの一方のビットを出力ビットとして採用する。

【0010】

このほかの本発明の特徴ならびに利点は、添付の図面および以下の詳細な説明から逐次明らかなものとなろう。

【0011】

なお、添付図面には、限定の意味ではなく、例示のための手段として本発明が

示されており、それらにおいては、類似の要素に類似の参照番号が用いられている。

【0012】

（詳細な説明）

乱数発生器内で使用するデューティ・サイクル修正器を説明する。一実施形態においては、このデューティ・サイクル修正器によって、ランダム・ビット・ソースから出力されたビットの連続するペアが処理される。ビットのペアを構成する2つのビットがまったく等しい場合には、デューティ・サイクル修正器によってそのビットのペアが破棄されるか、あるいは出力されない。ビットのペアを構成する2つのビットが互いに異なる場合には、デューティ・サイクル修正器によってビット・ペア内のビットの一方が出力される。

【0013】

本発明の実施形態の利点として意図されていることは、ランダム・ビット・ソースの出力に関してほぼ一様なデューティ・サイクルを生成する回路を提供することである。さらに、集積回路デバイス内に実装された場合に、必要とするシリコン面積が小さい乱数発生器を提供することも本発明の実施形態の利点として意図されている。

【0014】

ここで、ランダム・ビット・ソースは、ランダムと推定される順序でバイナリ・ディジット系列を出力するデジタル回路であることを思い出されたい。理想的なランダム・ビット・ソースにおいては、所定の出力ビットが「0」となる確率が、それが「1」となる確率に等しい。つまり、ランダム・ビット・ソースの出力波形のデューティ・サイクルは、統計的に有意な標本サイズにわたって一様に50パーセントとなる。しかしながら、ほとんどのランダム・ビット・ソースは、禁止されたホールドタイムまたはセットアップタイムの間にデータがラッチされると、ランダム・ビット・ソース内のラッチならびにゲートが特定の論理・レベルをラッチするという傾向に起因したデューティ・サイクルの変動を呈する。

【0015】

ランダム・ビット・ソースによって特定時に所定のビットが出力される確率は、一定の数学的関係によって表すことができる。たとえば、出力が「0」になる確率 $P(0)$ を p とすれば、出力が「1」となる確率 $P(1)$ は $1-p$ で表される。すなわち、

「0」を生成する確率: $P(0) = p$

「1」を生成する確率: $P(1) = 1-p$

である。理想的なランダム・ビット・ソースにおいては、 p が 50 パーセントになる。逆に、理想的でないランダム・ビット・ソースの場合は、 p が 50 パーセントより実質的に大きくなるか、あるいはそれより小さくなる。

【0016】

ランダム・ビット・ソースの連続する出力をペアとして考えると、この確率は次のようになる。

「0」「0」を生成する確率: $P(00) = P(0)P(0) = p^2$

「0」「1」を生成する確率: $P(01) = P(0)P(1) = p(1-p)$

「1」「0」を生成する確率: $P(10) = P(1)P(0) = (1-p)p$

「1」「1」を生成する確率: $P(11) = P(1)P(1) = (1-p)^2$

【0017】

数学的に、「0」「1」の出力ペアと「1」「0」の出力ペアが生成される確率は、上記の確率の式からもわかるように、互いに等しい。つまり、 $p(1-p) = (1-p)p$ であり、したがって $P(01) = P(10)$ である。

【0018】

この性質は、ランダム・ビット・ソースが「1」を生成する確率、または「0」を生成する確率とは無関係に、与えられた任意の出力に関して真となる。したがって、特定のランダム・ビット・ソースについて、 p が 50 パーセントとならない場合であっても、そのランダム・ビット・ソースが「0-1」の出力ペアを生成する確率は、それが「1-0」の出力ペアを生成する確率に等しい。本発明の一実施形態においては、この原理を用いて、一様でないデューティ・サイクルを呈し、かつ所定の出力ビット・ストリーム内の「0」と「1」の分布が一様でないランダム・ビット・ソースの出力を訂正する。

【0019】

本発明の1つの方法においては、デューティ・サイクル修正器がランダム・ビット・ソースから出力されたペアとなるビットを処理して、修正した、実質的にデューティ・サイクルが一般的なビット・ストリームを決定する。一実施形態においては、ビットのペアを構成するビットがともに等しいときには、デューティ・サイクル修正器によってそのペアが破棄され、修正後のビット・ストリームの一部として出力されない。つまり、出力ビットのペアを構成するビットがともに「0」であれば、そのペアが破棄される。それと同様に、出力ビットのペアを構成するビットがともに「1」であれば、そのペアが破棄される。しかしながら、出力ビットのペアを構成するビットが互いに異なれば、デューティ・サイクル修正器により、そのペアの一方のビットが修正後のビット・ストリームの1つのビットとして出力される。一実施形態においては、デューティ・サイクル修正器が異なるビットからなるペア内の最初のビットを修正後のビットとして出力する。したがって、この実施形態においては、出力ペアが「0-1」であれば修正後のビットが「0」にセットされ；出力ペアが「1-0」であれば修正後のビットが「1」にセットされる。各種のペアの場合に対応する修正後のビット値は、次の関係を用いて表すことができる。

$$\begin{aligned} P(00) &= P(0)P(0) = p^2 && \text{破棄される} \\ P(01) &= P(0)P(1) = p(1-p) && \text{論理「0」が出力される} \\ P(10) &= P(1)P(0) = (1-p)p && \text{論理「1」が出力される} \\ P(11) &= P(1)P(1) = (1-p)^2 && \text{破棄される} \end{aligned}$$

【0020】

変形実施形態においては、デューティ・サイクル修正器が異なるビットからなるペア内の2番目のビットを修正後のビットとして出力する。つまり、この実施形態においては、出力ペアが「0-1」であれば修正後のビットが「1」にセットされ；出力ペアが「1-0」であれば修正後のビットが「0」にセットされる。したがって、この変形実施形態における各種のペアの場合に対応する修正後のビット値は、次の関係を用いて表すことができる。

$$P(00) = P(0)P(0) = p^2 \quad \text{破棄される}$$

$P(01) = P(0)P(1) = p(1-p)$ 論理「1」が出力される

$P(10) = P(1)P(0) = (1-p)p$ 論理「0」が出力される

$P(11) = P(1)P(1) = (1-p)^2$ 破棄される

【0021】

図2は、上記の実施形態を具体化したデューティ・サイクル修正器200の一実施形態を示しており、それにおいては、ランダム・ビット・ソース202の出力から実質的に一様なビット・ストリームが生成され、しかも従来のLFSR回路より使用されているゲート数が少ない。ランダム・ビット・ソース202は、信号ライン222上にランダムなビットのストリームを出力するものであれば、任意のランダム・ビット・ソースとすることができる。本発明の一実施形態においては、ランダム・ビット・ソース202が、高速発振信号を周期的にラッチするランダムに変化させた低速クロック信号を使用するラッチ回路として実装される。ランダム・ビット・ソースのラッチから出力されるビットの値は、低速信号によってラッチされたときの高速信号の電圧レベルに依存する。またランダム・ビット・ソース202は、この分野において一般に知られているように、クロック信号またはストロブ信号CLKを生成して信号ライン216上に供給する。

【0022】

デューティ・サイクル修正器200は、ストレージ・エレメント204と206、比較回路208、確認論理210、および出力回路212を含んでいる。ストレージ回路204と206は、ランダム・ビット・ソース202から出力されたランダム・ビット・ストリーム内の連続するビットをペアとして、比較回路208による比較のためにストアする。CLKの第1のクロック・サイクルにおいて、ペアとなるビットの最初のビットがストレージ回路204にストアされる。この最初のビットは、続くクロック・サイクルにおいてストレージ回路206にストアされ、ストレージ回路204には、そのときランダム・ビット・ソース202から出力された次のビットがストアされる。ストレージ回路204と206は、ラッチ、レジスタ、揮発性もしくは不揮発性メモリ・セル、およびその他の等価物を含めた任意のタイプのストレージ・エレメントとすることができる。

【0023】

ストレージ回路204と206にストアされたビットは、比較回路208によって比較される。この比較回路208は、エクスクルーシブオア・ゲートもしくはコンパレータといった任意のタイプの比較回路とすることができる。2つのビットが等しいときには、比較回路208が、信号ライン220上の信号を論理ハイの状態にセットしてACCEPT（アクセプト）をアサートする。2つのビットが等しくないときには、比較回路208が、その信号を論理ローの状態にセットしてACCEPT（アクセプト）のアサートを解く。つまり、ACCEPT（アクセプト）信号は、ランダム・ビット・ソースから出力されるペアとなるビットが、デューティ・サイクル修正器200によって出力されるビット・ストリーム内の修正後のビットとなり得るか否かを示すことになる。

【0024】

ACCEPT（アクセプト）信号は、CLKとともに確認論理210に渡される。比較回路208は、ストレージ回路204と206内の連続する2つのビットが互いに異なるとき、ACCEPT（アクセプト）をアサートする。しかしながら、デューティ・サイクル修正器200が一樣なデューティ・サイクルの出力ストリームを生成するためには、ランダム・ビット・ソース202から出力されるビットをオーバーラップさせることなく比較する方が好ましい。その機能を具体化している部分が確認論理210である。確認論理210は、ACCEPT（アクセプト）がアサートされ、かつ望ましいビットのペアがストレージ回路204と206にストアされているとき、信号ライン218上の信号を論理ハイの状態にセットしてストロブ信号STBをアサートする。STBがアサートされると、出力回路212がストレージ回路206内のビットをストアする。出力回路212は、レジスタ、ラッチ、1ないしは複数の揮発性もしくは不揮発性メモリ・エレメント、アンド・ゲート、あるいはその他の論理を含めて任意のストレージ・エレメントとすることができる。出力回路212によってストアされたビットは、ストレージ回路204と206内にストアされたビットに対応する修正後のビットとして信号ライン214に出力される。

【0025】

変形実施形態に関しては、ストレージ回路206の出力に代えてストレージ回

路204の出力を出力回路212に渡すことができる。その実施形態の場合、STBがアサートされると出力回路212がストレージ回路204内のビットをストアし、このビットをストレージ回路204と206内にストアされたビットに対応する修正後のビットとして出力する。

【0026】

図3は、デューティ・サイクル修正器200の一実施形態であるデューティ・サイクル修正器300を示している。デューティ・サイクル修正器300は、ストレージ回路204と206のそれぞれ一実施形態であるラッチ304および306；比較回路210の一実施形態であるエクスクルーシブ・オア・ゲート310；確認論理210の一実施形態であるトランスペアレント・ラッチ308およびアンド・ゲート309の組み合わせ；および出力回路212の一実施形態であるラッチ312を含んでいる。

【0027】

ラッチ304および306は、ランダム・ビット・ソース202から出力された連続するビットをペアとして、エクスクルーシブ・オア・ゲート310による比較のためにストアする。ペアとなるビットの最初のビットが、CLKによってラッチ304内にラッチされる。CLKの次のクロック・パルスでは、この最初のビットがラッチ306にラッチされ、ランダム・ビット・ソース202から出力された次のビットがラッチ304内にラッチされる。ビットのペアを構成する2つのビットが等しければ、エクスクルーシブ・オア・ゲート310がACCEPT（アクセプト）のアサートを行わずに「0」を出力し；ビットのペアを構成する2つのビットが互いに異なれば、エクスクルーシブ・オア・ゲート310が「1」を出力してACCEPT（アクセプト）をアサートする。

【0028】

トランスペアレント・ラッチ308は、ランダム・ビット・ソース302からのCLKをラッチし、ACCEPT（アクセプト）がアサートされ、かつラッチ304および306にオーバーラップのないビットのペアがストアされているときにSTBがアサートされるようにアンド・ゲート309をクロックする。STBがアサートされると、ラッチ312がラッチ306から出力されたビットを、

信号ライン 2 1 4 上に出力する修正後のビットとしてラッチする。別の実施形態においては、ラッチ 3 0 4 の出力をラッチ 3 1 2 に供給することができる。このビットを、ラッチ 3 1 2 により S T B に応答してラッチすればよい。

【0029】

図 4 は、デューティ・サイクル修正器 3 0 0 の動作を示したフローチャートである。ステップ 4 0 0 において、ラッチ 3 0 4 および 3 0 6 がランダム・ビット・ソース 2 0 2 から最初のペアとなるビットをラッチするが、そのうちの最初のビットはラッチ 3 0 6 にストアされ、2 番目のビットはラッチ 3 0 4 にストアされる。ステップ 4 0 2 においては、エクスクルーシブ・オア・ゲート 3 1 0 が、ペアを構成する 2 つのビットが等しいか否かを決定する。ペアを構成する 2 つのビットが等しいときには、ステップ 2 0 4 において、A C C E P T (アクセプト) のアサートおよび S T B のアサートが行なわれることなく、このビットのペアが拒絶または破棄される。ステップ 2 0 4 においては、いずれのビットもラッチ 3 1 2 によってラッチされることがなく、また信号ライン 2 1 4 に出力されることもない。しかしながら、ステップ 4 0 2 において 2 つのビットが互いに異なると判断されると、ステップ 4 0 6 においてペア内の最初のビットが出力として獲得される。

【0030】

ステップ 4 0 8 においては、続くオーバーラップするペアとなるビットがランダム・ビット・ソース 2 0 2 から取り込まれ、その後プロセスがステップ 4 0 2 から繰り返される。このプロセスは、ランダム・ビット・ソースからの出力ビットのペアがすべて処理されるまで繰り返される。ペアを構成しない乱数源からの出力ビットは、処理不可能であり、したがって破棄される。ここでは、ペアを構成する最初のビットがラッチ 3 0 6 から修正後のビットとして供給されているが、別の方法においては、修正後のビットとして、ペアを構成する 2 番目のビットをラッチ 3 0 4 から供給できることに注意する必要がある。

【0031】

図 5 は、デューティ・サイクル修正器 3 0 0 の動作をさらに別の形で説明している。図 5 を参照すると、2 番目のペアとなるビット (ビット 2 および 3) およ

び3番目のペアとなるビット（ビット4および5）は修正後のビットを生成するが、最初のペアとなるビット（ビット0および1）および4番目のペアとなるビット（ビット6および7）からは生成されないことがわかる。

【0032】

ランダム・ビット・ソース202は、ラッチ、論理ゲート、およびその他の回路エレメントの特性に起因して、連続的に生成されたビットの間に1次の自己相関を有するビットを出力することがある。つまり、図2および3に示したような上記のデューティ・サイクル修正器が実質的に一様なデューティ・サイクルを有するランダム・ビット・パターンを実質的に出力できる場合であっても、ランダム・ビット・ソースによって出力されるビット間の自己相関が低くないとデューティ・サイクル修正器の出力が一様なデューティ・サイクルに近づく可能性が高くなる。言い換えれば、ランダム・ビット・ストリーム内のビットが互いに相関を有していない場合においては、デューティ・サイクル修正器の出力が一様なデューティ・サイクルに近づく可能性が高くなる。

【0033】

図5に示されるように、図3に示したデューティ・サイクル修正器300は、ビットの連続するペアに対してデューティ・サイクル修正器300が作用することから、ランダム・ビット・ソース202によって出力されたランダム・ビット・ストリーム内のビット間における1次の自己相関による影響を受けることがあり得る。図6は、別の実施形態、すなわちランダム・ビット・ソース202によって出力されるビットのペアの間における1次の自己相関の影響を軽減するデューティ・サイクル修正器600を示している。このデューティ・サイクル修正器600は、修正後のビットを生成したビットのペアが検出されるごとに、ランダム・ビット・ソース202から出力されるビットを1つ破棄することによって1次の自己相関の影響を軽減する。

【0034】

デューティ・サイクル修正器600は、デューティ・サイクル修正器300に類似であるが、確認論理のトランスペアレント・ラッチ308がモジュロ2カウンタ602に置き換えられている点異なる。デューティ・サイクル修正器60

0の動作を図7に示す。ステップ700においては、モジュロ2カウンタ602のカウンタ「0」と「1」にตอบสนองして、ラッチ304および306がランダム・ビット・ソース202からの最初のペアとなるビットをラッチする。ステップ702においては、エクスクルーシブオア・ゲート310が、ペアを構成する2つのビットが等しいか否かを決定する。ペアを構成する2つのビットが等しいときには、ステップ704において、ACCEPT（アクセプト）のアサートおよびSTBのアサートが行なわれることなく、このビットのペアが拒絶または破棄される。ステップ704においては、いずれのビットもラッチ312によってラッチされることがなく、また信号ライン214に出力されることもない。しかし、ステップ702において2つのビットが互いに異なると判断されると、ステップ704において、カウンタ「1」にตอบสนองしてACCEPT（アクセプト）がアサートされ、STBがアサートされて、ラッチ312により最初のビット（または、それに代えて2番目のビット）が出力される。このSTBは、モジュロ2カウンタ602にもフィードバックされ、その結果、STBがアサートされるとモジュロ2カウンタ602が1カウントをスキップし、次の2クロック・サイクルをローに（つまり両方をカウンタ「0」に）保持する。これによりステップ807において、デューティ・サイクル修正器600は、ランダム・ビット・ソース202からのランダム・ビット・ストリーム内の次のビットを破棄する。この「次のビット」はラッチ304内にロードされているが、モジュロ2カウンタ602が次にアンド・ゲート309に対してカウンタ「1」を出力する前に、クロックされてラッチ306を通り抜けることからこれが可能になる。ステップ708においては、続くオーバーラップするペアとなるビットがランダム・ビット・ソース202から取り込まれ、その後プロセスがステップ702から繰り返される。このプロセスは、ランダム・ビット・ソースからの出力ビットのペアがすべて処理されるまで繰り返される。

【0035】

デューティ・サイクル修正器600の動作を別の形で図8に示す。最初のペアとなるビット（ビット0および1）の処理時においては、ペア内のビットが等しいことから破棄され、このビットのペアに関しては修正後のビットが生成されな

い。それに加えて、STBのアサートがないことからモジュロ2カウンタ602によるカウントのスキップも行なわれない。2番目のペアとなるビット（ビット2および3）はビット値が異なることから、デューティ・サイクル修正器600が「0」を出力し、続いてモジュロ2カウンタ602がカウントをスキップすることから、その次のビット、つまりビット4が破棄される。3番目のペアとなるビット（ビット5および6）もビット値が等しくない。その結果、デューティ・サイクル修正器600が「1」を出力し、モジュロ2カウンタ602がカウントをスキップすることから、その次のビット、つまりビット7が破棄される。最後のペアとなるビット（ビット8および9）は、ビット値が等しいことから破棄される。

【0036】

ビット4および7を破棄することによって2番目のビットのペア（ビット2および3）と3番目のビットのペア（ビット5および6）の間の1次の自己相関、および3番目のビットのペアと4番目のビットのペア（ビット8および9）の間の1次の自己相関が低減される。修正後のビット・ストリームは、ランダム・ビット・ソース202によって出力された2番目のビットのペアと3番目のビットのペアの間、および3番目のビットのペアと4番目のビットのペアの間における2次の自己相関の影響を受けるが、その有意性はあまり高くない。

【0037】

デューティ・サイクル修正器600は、ランダム・ビット・ソースによって生成されたビットの間における1次の自己相関を低減する。しかしながら、それぞれの破棄されるビット（たとえば図8のビット4および7）がランダム・ビット・ストリーム内に一様に分布していないことから、修正後のビット・ストリームのデューティ・サイクルに非一様性が招かれる傾向を否定できない。

【0038】

図9は、さらに別の実施形態、すなわちランダム・ビット・ソース202によって出力されるビットのペアの間における1次の自己相関の影響を軽減するデューティ・サイクル修正器900を示している。デューティ・サイクル修正器900は、ランダム・ビット・ソース202の、モジュロ5カウンタの特定のカウン

トに応じてシフトインされたビットを破棄することによって、1次の自己相関を低減する。

【0039】

デューティ・サイクル修正器900は、デューティ・サイクル修正器300に類似であるが、確認論理のトランスペアレント・ラッチ308が、モジュロ5カウンタ902、インバータ904、906、908、アンド・ゲート910、912、およびノア・ゲート914に置き換えられている点異なる。モジュロ5カウンタ902は、3つのバイナリ出力ビットC0、C1、C2を有している。アンド・ゲート910は、3入力アンド・ゲートであり、第1の入力がインバータ904を介してC2に結合され、第2の入力がC1に結合され、第3の入力がインバータ908を介してC0に結合されている。アンド・ゲート912は、3入力アンド・ゲートであり、第1の入力がC2に結合され、第2の入力がインバータ906を介してC1に結合され、第3の入力がインバータ908を介してC0に結合されている。ノア・ゲート914は、アンド・ゲート910および912の出力を受け取り、アンド・ゲート309の一方の入力をドライブする。

【0040】

デューティ・サイクル修正器900の動作を図10に示す。ステップ1000およびモジュロ5カウンタ902のカウント「0」において、最初のビットがラッチ304にロードされる。カウント「0」と「1」については、信号ライン915上に信号がアサートされないことから、このビットは破棄される。ステップ1002においては、カウント「1」と「2」にตอบสนองして、最初のペアとなるビットがランダム・ビット・ソース202からラッチ304および306にラッチされる。このラッチが、修正器1000に最初のビットを破棄させる。ステップ1004およびカウント「2」においては、エクスクルーシブオア・ゲート310が、ペアを構成する2つのビットが等しいか否かを判断する。ペアとなるビットが等しいときには、ステップ1006において、ACCEPT（アクセプト）のアサートおよびSTBのアサートが行なわれることなく、このビットのペアが拒絶または破棄される。ステップ1006においては、いずれのビットもラッチ312によってラッチされることがなく、また信号ライン214に出力される

こともない。ステップ1004およびカウント「2」において、2つのビットが互いに異なると判断されると、ステップ1008においてACCEPT（アクセプト）がアサートされ、STBがアサートされて、ラッチ312によりペア内の最初のビット（または、それに代えて2番目のビット）が出力される。

【0041】

ステップ1010においては、カウント「3」および「4」に応答して、2番目のペアとなるビットがランダム・ビット・ソース202からラッチ304および306にラッチされる。ステップ1012およびカウント「4」においては、エクスクルーシブオア・ゲート310が、ペアを構成する2つのビットが等しいか否かを判断する。ペアとなるビットが等しいときには、ステップ1014において、ACCEPT（アクセプト）のアサートおよびSTBのアサートが行なわれることなく、このビットのペアが拒絶または破棄される。ステップ1012およびカウント「4」において、2つのビットが互いに異なると判断されると、ステップ1016においてACCEPT（アクセプト）がアサートされ、STBがアサートされて、ラッチ312によりペア内の最初のビット（または、それに代えて2番目のビット）が出力される。このプロセスが、ランダム・ビット・ソースから出力されるすべてのビットのペアに対する処理を完了するまで繰り返される。

【0042】

図11は、デューティ・サイクル修正器900の動作をさらに別の形で示している。最初のビット、すなわちビット0は、修正器900にロードされるが、最初のペアとなるビットがロードされるときに破棄される。最初のペアとなるビット（ビット1と2）は、ビット値が等しいことから破棄され、このビットのペアに関しては修正後のビットが生成されない。2番目のペアとなるビット（ビット3と4）はビット値が異なることから、デューティ・サイクル修正器900が「0」を出力する。その後、モジュロ5カウンタ902のカウントが「0」に戻り、その結果、ビット5が破棄される。3番目のペアとなるビット（ビット6と7）もビット値が異なり、デューティ・サイクル修正器900は「1」を出力する。最後のペアとなるビット（ビット8および9）はビット値が互いに等しく、し

たがって破棄される。

【0043】

ビット0と5を破棄することによって2番目のビットのペア（ビット3と4）と3番目のビットのペア（ビット6と7）の間の1次の自己相関が低減される。修正後のビット・ストリームは、2番目のビットのペアと3番目のビットのペアの間における2次の自己相関の影響を受けるが、その有意性はあまり高くない。カウント「0」（カウント「5」、カウント「10」等）で破棄されるビットは、ランダム・ビット・ストリーム内に一様に分布し、それらを除外しても、結果的に修正後のビット・ストリームに関するデューティ・サイクルは概略で一様になる。

【0044】

図12は、さらに別の実施形態、すなわちランダム・ビット・ソース202によって出力されるビットのペアの間における1次の自己相関の影響を軽減するデューティ・サイクル修正器1200を示している。デューティ・サイクル修正器1200は、ランダム・ビット・ソース202が出力したビットから、比較されるビットのペアの間に挟まれるビットを破棄することによって1次の自己相関を抑える。

【0045】

デューティ・サイクル修正器1200は、デューティ・サイクル修正器300に類似であるが、確認論理のトランスペアレント・ラッチ308が、カウント「2」のときにのみ信号ライン1204上に論理ハイの信号を出力するモジュロ3カウンタ1202に置き換えられている点異なる。

【0046】

デューティ・サイクル修正器1200の動作を図13に示す。ステップ1300およびモジュロ3カウンタ902のカウント「0」において、最初のビットがラッチ304にロードされる。カウント「0」と「1」については、信号ライン1204上に信号がアサートされないことから、このビットは破棄されることになる。ステップ1302においては、カウント「1」と「2」にตอบสนองして、最初のペアとなるビットがランダム・ビット・ソース202からラッチ304および

306にラッチされる。このラッチによって、修正器1200が最初のビットを破棄する。ステップ1304およびカウント「2」においては、エクスクルーシブオア・ゲート310が、ペアを構成する2つのビットが等しいか否かを判断する。ペアとなるビットが等しいときには、ステップ1306において、ACCEPT（アクセプト）のアサートおよびSTBのアサートが行なわれることなく、このビットのペアが拒絶または破棄される。ステップ1306においては、いずれのビットもラッチ312によってラッチされることがなく、また信号ライン214に出力されることもない。ステップ1304およびカウント「2」において、2つのビットが互いに異なると判断されると、ステップ1308においてACCEPT（アクセプト）がアサートされ、STBがアサートされて、ラッチ312によりペア内の最初のビット（または、それに代えて2番目のビット）が出力される。このプロセスが、ランダム・ビット・ソースからの出力ビットのペアがすべて処理されるまで繰り返される。

【0047】

図14は、デューティ・サイクル修正器1200の動作をさらに別の形で示している。最初のビット、すなわちビット0は、修正器1200にロードされるが、最初のビットのペアがロードされるとき破棄される。最初のペアとなるビット（ビット1と2）の処理時においては、ペア内のビットが等しいことから破棄され、このビットのペアに関しては修正後のビットが生成されない。4番目のビット、すなわちビット3は、修正器1200にロードされるが、2番目のペアとなるビットがロードされるとき破棄される。2番目のペアとなるビット（ビット4と5）はビット値が異なることから、修正器1200が「0」を出力する。7番目のビット、すなわちビット6は、修正器1200にロードされるが、3番目のペアとなるビットがロードされるとき破棄される。3番目のペアとなるビット（ビット7と8）はビット値が異なり、デューティ・サイクル修正器1200は「1」を出力する。10番目のビット、すなわちビット9は、修正器1200にロードされるが、4番目のペアとなるビットがロードされるとき破棄される。4番目のペアとなるビット（ビット10と11）は、ビット値が等しいことから破棄される。

【0048】

ビット0、3、6、9等を破棄することによって、比較を行うビットのペアの間における1次の自己相関が低減される。修正後のビット・ストリームは、比較を行うビットのペアの間における2次の自己相関の影響を受けるが、その有意性はあまり高くない。モジュロ3カウンタ1202のカウント0、3、6、9等において破棄されるビットは、ランダム・ビット・ストリーム内に一様に分布し、それらを除外しても、結果的に修正後のビット・ストリームに関するデューティ・サイクルは概略で一樣になる。

【0049】

以上、ランダム・ビット・ソースのランダム・ビット・ストリーム内の連続する2つのビットを比較するものとしてデューティ・サイクル修正器の説明を行ってきたが、変形実施形態として、連続しないビットを比較することもできる。たとえば、ストレージ回路204と206の間に追加のストレージ回路を挿入し、あるいはそれぞれのストレージ回路を異なるクロックもしくは異なるクロック・エッジを用いてクロックすることが考えられる。

【0050】

また、ここで説明した出力回路212は、ストレージ回路204と206のうちのいずれか一方の出力を受け取る。変形実施形態においては、比較論理208に、ストレージ回路204と206にストアされているデータに応答して出力回路212に提供されるデータを決定する論理を含めることができる。

【0051】

ランダム・ビット・ソースから実質的に一樣な「1」と「0」の分布を生成するための、ここで説明したデューティ・サイクル修正器は、コンピュータ・ネットワークを介して送られるメッセージの符号化および復号化を行うための乱数発生器と組み合わせて使用することができる。図15は、上記のいずれかの実施形態を使用して暗号化されたメッセージを送信するためのコンピュータ・ネットワークを示したブロック図である。ネットワーク1500は、送信ホスト・コンピュータ1502およびネットワークを介してそれに結合された受信ホスト・コンピュータ1504を含んでいる。送信ホスト・コンピュータおよび受信ホスト・

コンピュータは、ともにネットワーク・インターフェース・デバイスを備え、それによってホスト・コンピュータ・システムとネットワーク・メディアの間の物理的かつ論理的な接続が提供される。さらにいずれのホスト・コンピュータにも暗号化回路／解読回路が備わり、それが、データ通信のセキュリティに関する各種の暗号機能を実行する。送信ホスト1502は、暗号化回路／解読回路1506を備えており、受信ホスト1504は、暗号化回路／解読回路1507を備えている。暗号化回路／解読回路1506および1507には、それぞれ乱数発生器1508および1509が備わり、そこには、図2、3、6、9、または12に示した実施形態のいずれかが採用されている。これらの乱数発生器は、公開キー／秘密キーシステムにおける公開キー／秘密キーの生成に使用される。

【0052】

ネットワーク1500においては、送信ホスト1502と受信ホスト1504の間の安全な通信を保証するために、各種のデータ暗号化方法を使用することができる。一実施形態においては、ネットワーク1500が公開キー（非対称）暗号システムを使用する。公開キーシステムにおいては、2つの異なるキーが使用される。一方のキーは、送信側がメッセージの符号化のために使用し、他方のキーは、受信側が符号化されたメッセージの復号化のために使用する。このシステムにおいては、暗号化（公開）キーは広く公開してもよいが、復号（秘密）キーは、意図された受信側だけがメッセージの復号化を行えるように秘密にする必要がある。公開キーおよび秘密キーは、通常、非常に大きな素数および乱数からともに導かれる。したがって、真にランダムなキーのペアを生成するためには、効果的な乱数発生器が必要になる。

【0053】

公開キーシステムを使用するデータ送信の例において、送信ホスト1502は、受信ホスト1504に送信するためのメッセージMを作成する。この伝送のために使用される2つのキーは、受信側の公開キー（ PuK_R ）および受信側の秘密キー（ PrK_R ）からなる。通常、受信側は、公に入手可能な登録キーから公開キーを選択し、受信側のみが知っている変換プロセスを介して、当該公開キーから秘密キーを導く。つまり、一般に公開キーと秘密キーの間の相関は、秘密で

あり、かつ安全である。送信ホスト1502は、公開キーを使用し、暗号化回路／解読回路1506を介してメッセージを符号化し、符号化済みのメッセージM'を生成する。符号化が行われた後は、適切な秘密キーを使用しない限りメッセージを復号化することができない。受信ホスト1504は、メッセージを受信すると、秘密キーを用いてメッセージM'の復号化を行い、オリジナルのメッセージMを取り出す。

【0054】

一実施形態においては、受信ホスト1504内の暗号化回路／解読回路1507が、図2、3、6、9、または12の実施形態のいずれかを採用した乱数発生器1509を備えている。このテクニックは、乱数発生器1509からのビットの分布が十分に一樣かつランダムであり、そのため公開キーと、受信ホスト1504によって生成される秘密キーの間に一貫性のある相関が存在しない。ネットワーク1500内に示されるように、送信ホスト1502内の暗号化回路／解読回路1506もまた、図2、3、6、9、または12の実施形態のいずれかを採用した乱数発生器1508を備えている。これにより送信ホスト1502は、公開キーによる送信を採用するときの、安全な秘密キーおよび公開キーの生成が可能になる。これらのキーのペアの生成には、秘密キーの網羅的でないサーチが極めて困難になるように高度のランダム性が要求される。

【0055】

別の実施形態においては、ネットワーク1500が単一キー（対称）システムを使用して、暗号機能を実行する。単一キーシステムの場合には、送信側と受信側が1つのキーを共有し、それを使用して送信側はメッセージの暗号化を行い、受信側は、符号化されたメッセージの解読をおこなう。このシステムの信頼性は、キーのセキュリティに依存する。したがって、第三者に知られることのない、送信側と受信側の間のみにおけるキーの開示のために安全なプロセスが必要になる。この実施形態においては、通常、メッセージ・トランザクションが異なるごとに異なるキーが使用される。つまり、各種のキーが生成されることから、あるメッセージ・トランザクションに使用されるキーが、別のメッセージ・トランザクションに使用されたキーから決定不可能であることが保証される必要がある。

このシステムの場合、ネットワーク 1500 の各ホスト・コンピュータ内の暗号化回路／解読回路において、乱数発生器が使用されてホスト・コンピュータ間で送信されるメッセージ・データの符号化および復号化を行うためのランダムなキーパターンが生成される。

【0056】

なお、ここでは単一キーおよび公開キー／秘密キー暗号システムとの関連から本発明の実施形態を説明したが、本発明の実施形態は、安全なコンピュータ・ネットワークのための、これ以外のタイプの暗号システムにも使用できることに注意する必要がある。さらに、図 15 に示した暗号化回路／解読回路は、安全なデータ送信システムにおけるメッセージの符号化および復号化、送信されたメッセージの認証、ディジタル署名の検証、およびその他の機能を含めた各種の暗号機能の実行に使用することができる。

【0057】

以上のとおり、一様なデューティ・サイクルの乱数発生器を作るための回路について説明した。ここでは、特定の具体例とする実施形態を参照して本発明についての説明を行ったが、特許請求の範囲に示される本発明の精神ならびに範囲はそれよりも広く、それから逸脱することなくこれらの実施形態に対して各種の修正ないしは変更を加え得ることは明らかである。したがって、明細書ならびに図面は、限定的意味ではなく例示と考える必要がある。

【図面の簡単な説明】

【図 1】

リニア・フィードバック・シフト・レジスタを使用する従来の乱数発生器を示した図である。

【図 2】

ランダム・ビット・ソースおよびデューティ・サイクル修正器の一実施形態を示したブロック図である。

【図 3】

図 2 に示したデューティ・サイクル修正器の一実施形態を示した論理図である。

【図 4】

図 2 に示したデューティ・サイクル修正器の動作を示したフローチャートである。

【図 5】

図 3 に示したデューティ・サイクル修正器によって生成される修正後のビット・パターンの一例を示している。

【図 6】

図 2 に示したデューティ・サイクル修正器の別の実施形態を示した論理図である。

【図 7】

図 6 に示したデューティ・サイクル修正器の動作を示したフローチャートである。

【図 8】

図 6 に示したデューティ・サイクル修正器によって生成される修正後のビット・パターンの一例を示している。

【図 9】

図 2 に示したデューティ・サイクル修正器の一実施形態を示した論理図である。

【図 10】

図 10 に示したデューティ・サイクル修正器の動作を示したフローチャートである。

【図 11】

図 9 に示したデューティ・サイクル修正器によって生成される修正後のビット・パターンの一例を示している。

【図 12】

図 2 に示したデューティ・サイクル修正器の一実施形態を示した論理図である。

【図 13】

図 12 に示したデューティ・サイクル修正器の動作を示したフローチャートで

ある。

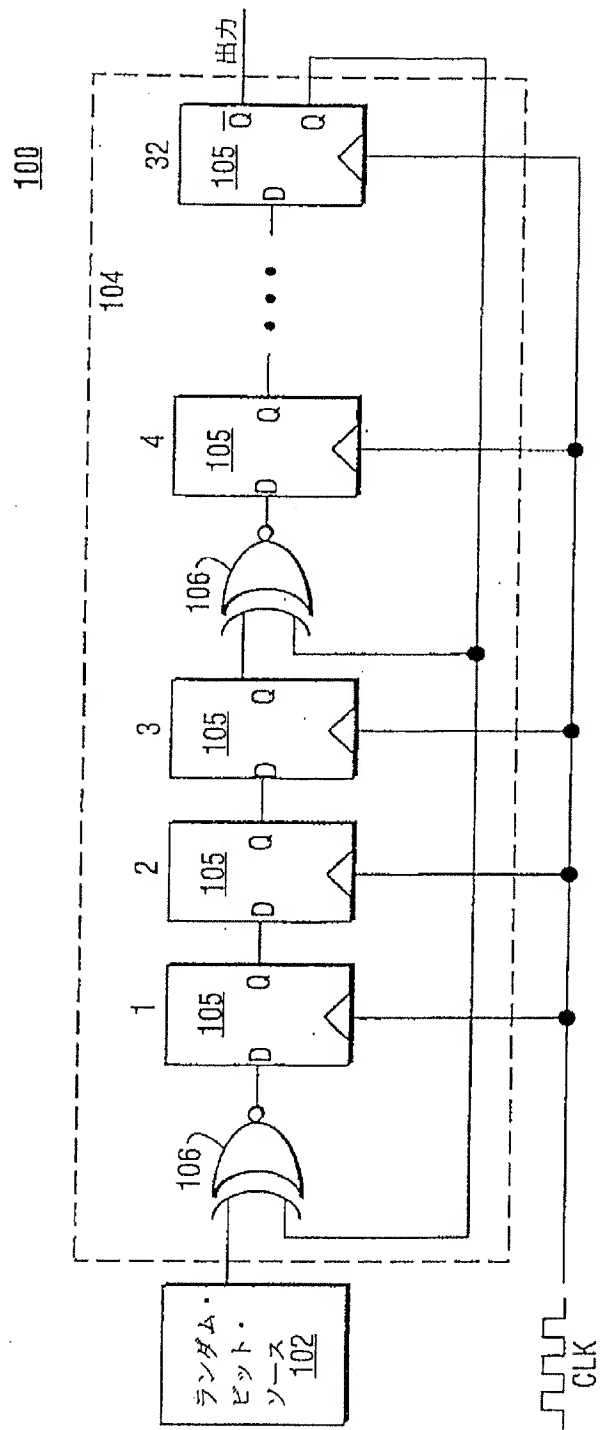
【図 1 4】

図 1 2 に示したデューティ・サイクル修正器によって生成される修正後のビット・パターンの一例を示している。

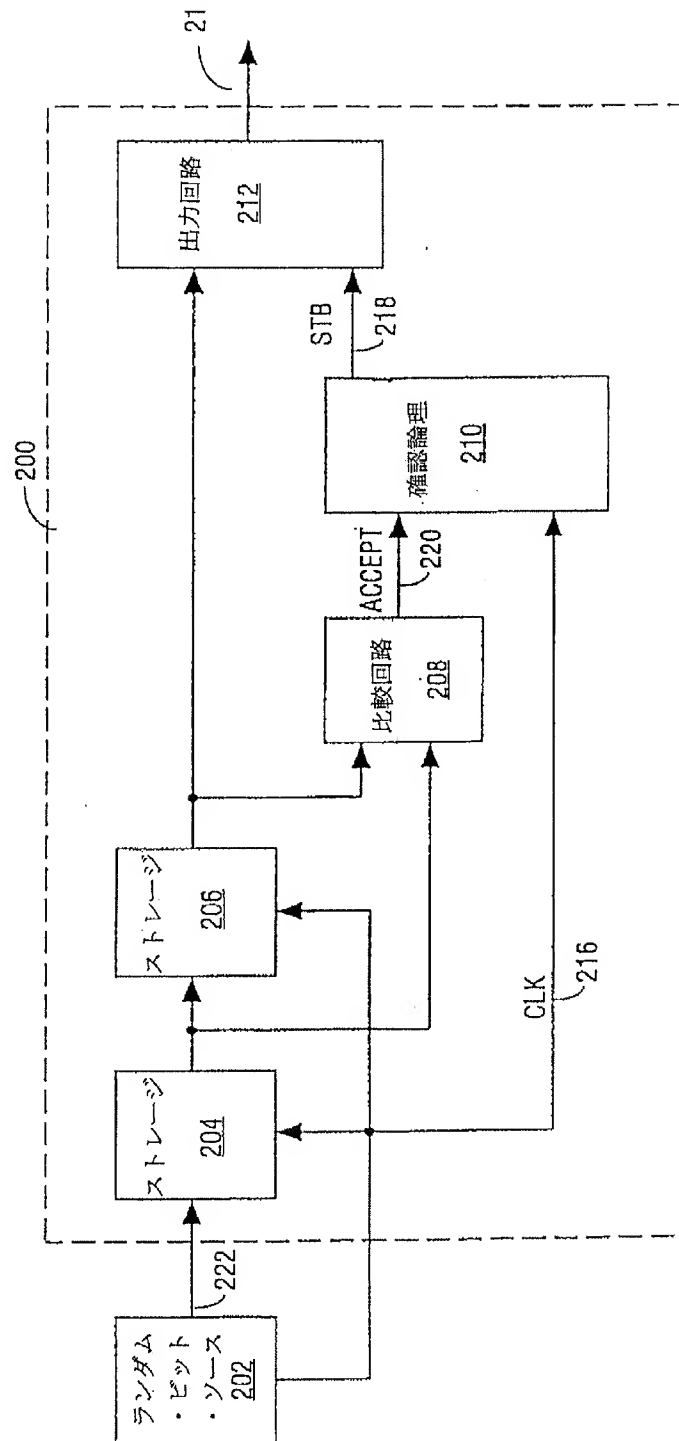
【図 1 5】

本発明の一実施形態に従ったデータ暗号化／解読のためのビット・ペアリング・システムを使用するコンピュータ・ネットワークを示したブロック図である。

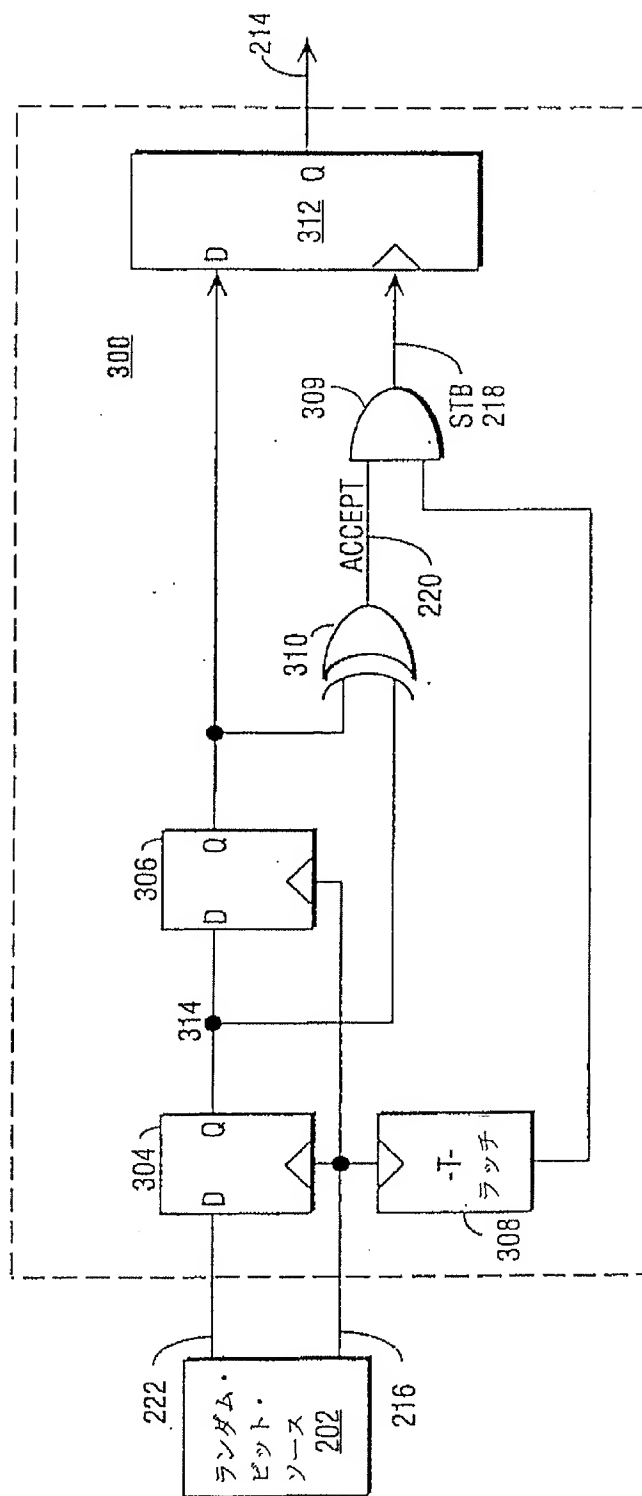
【図1】



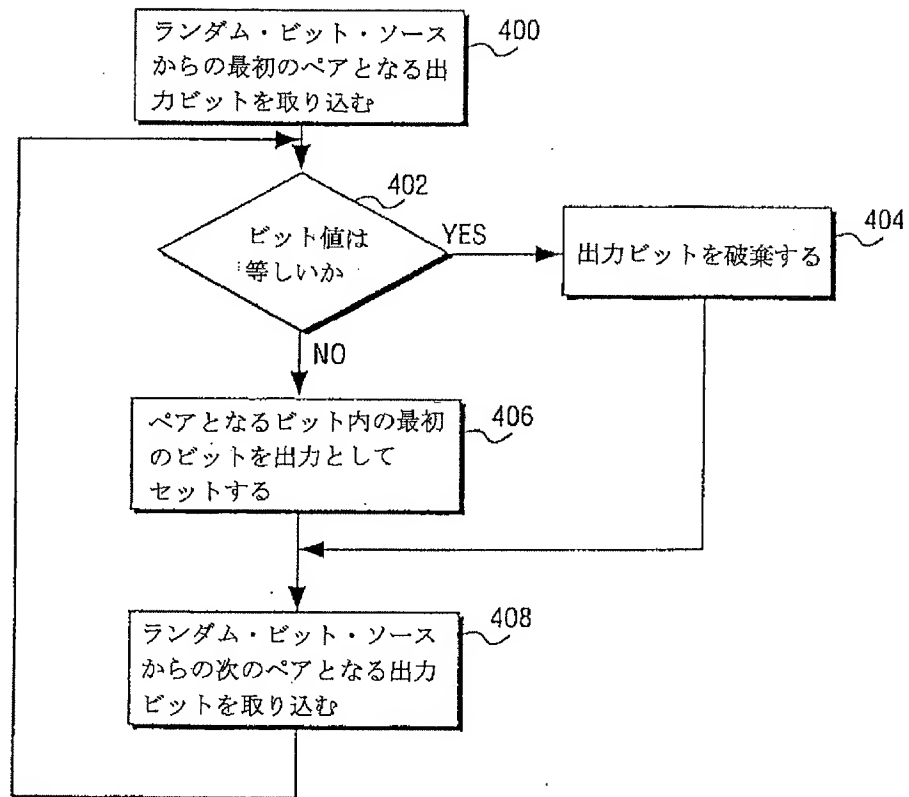
【図2】



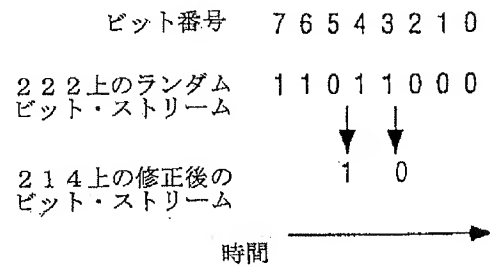
【図3】



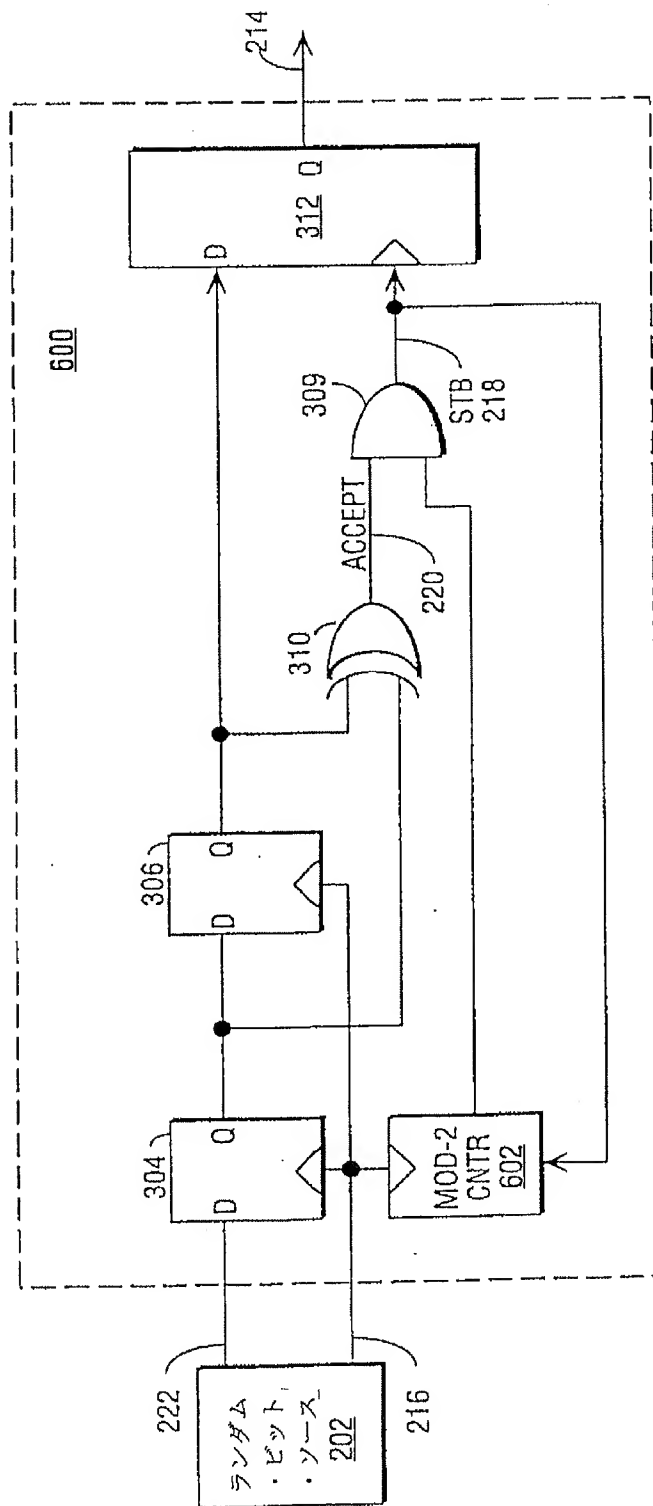
【図4】



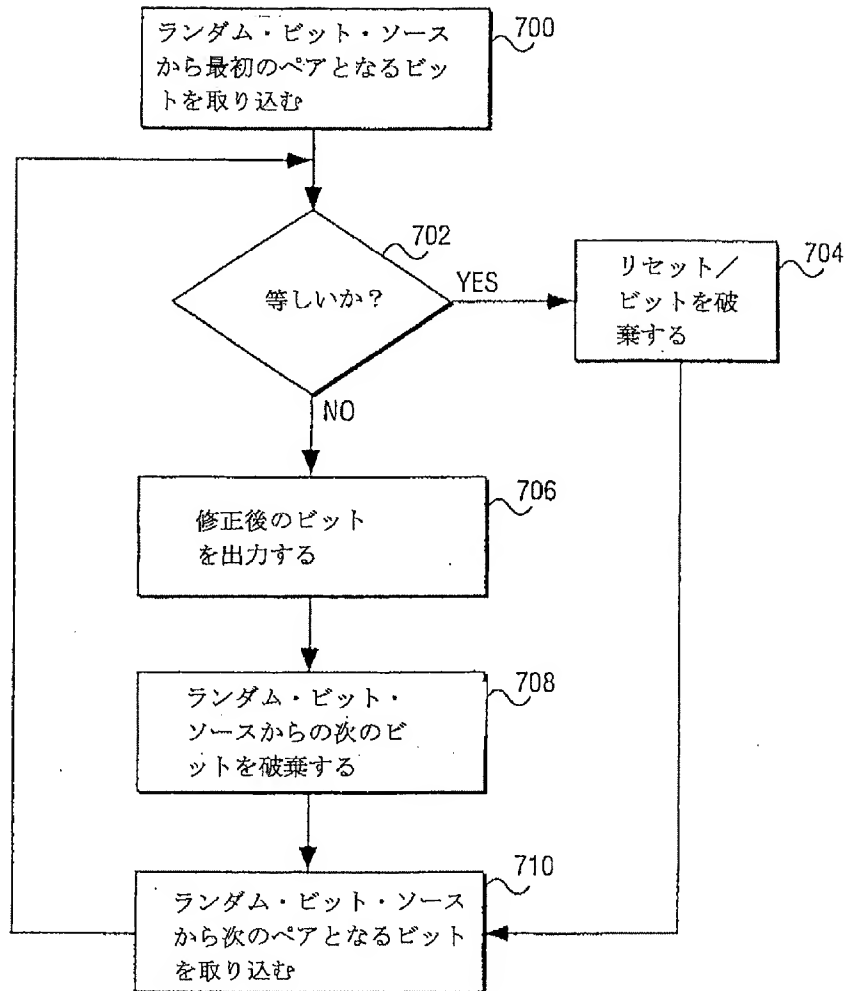
【図5】



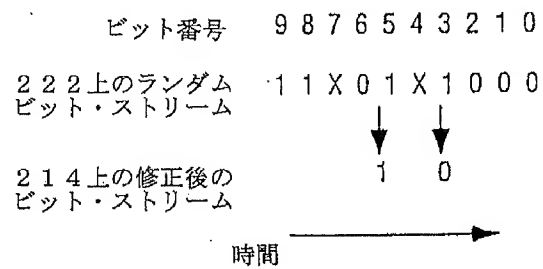
【図6】



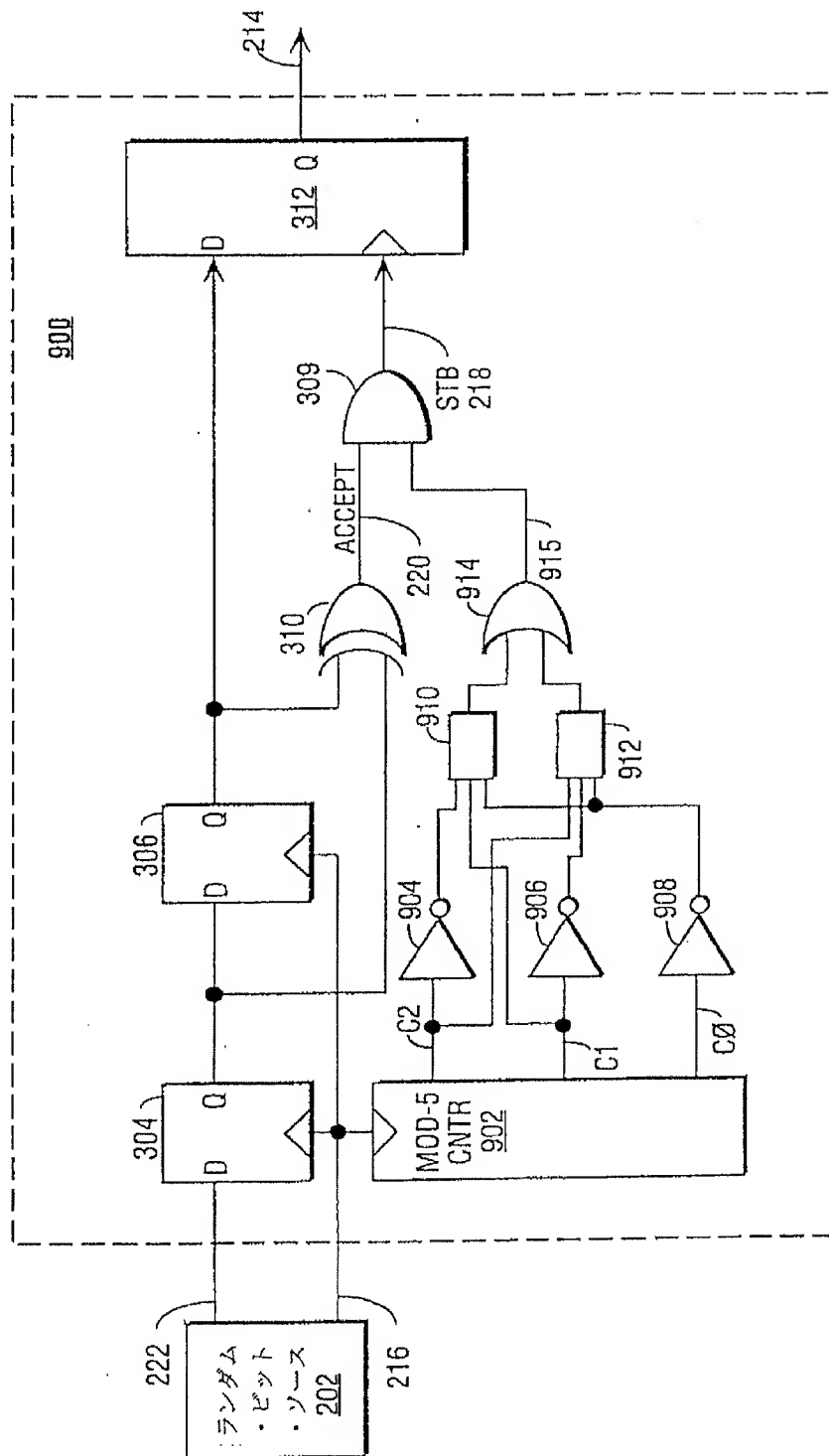
【図7】



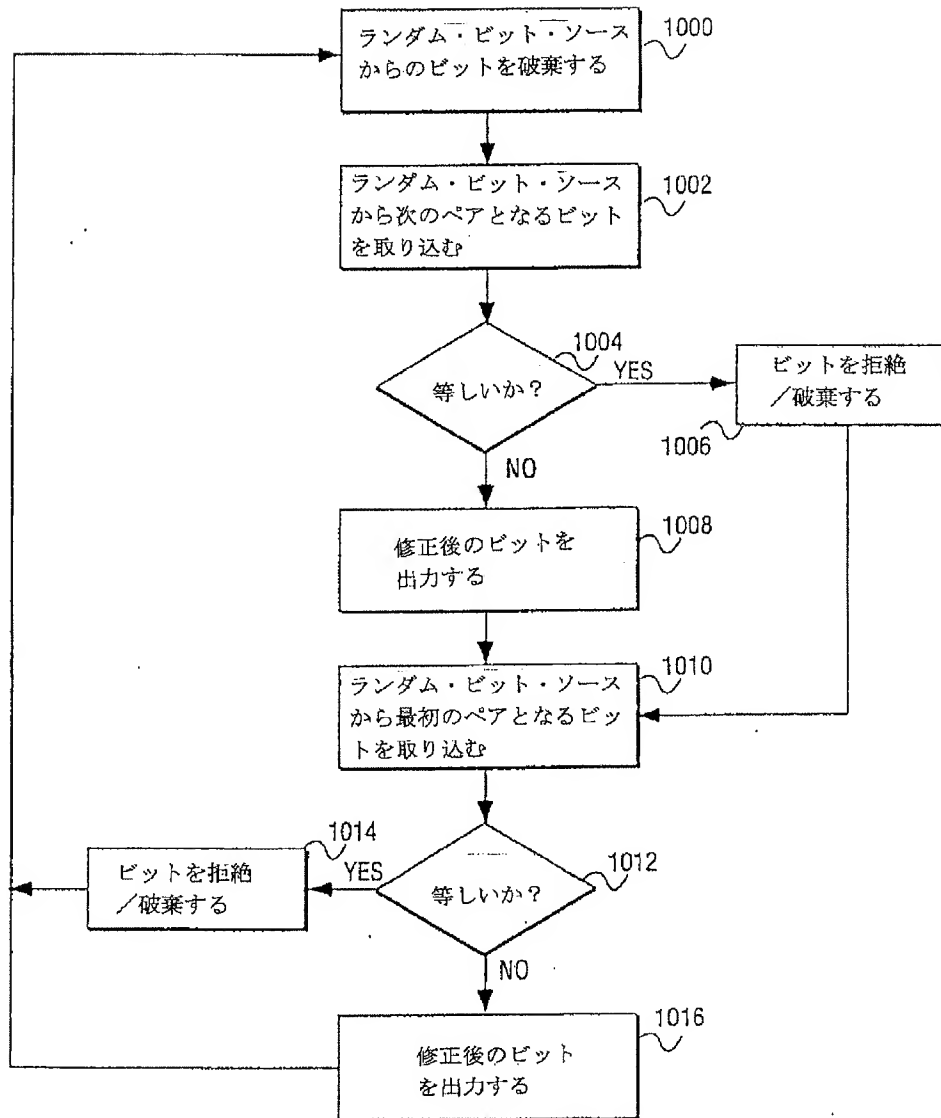
【図8】



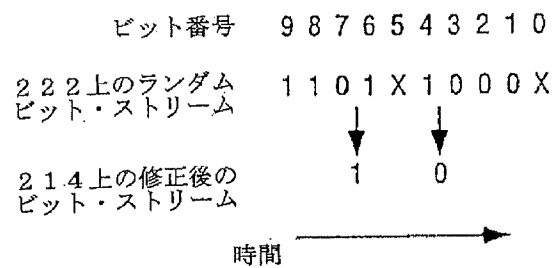
【図9】



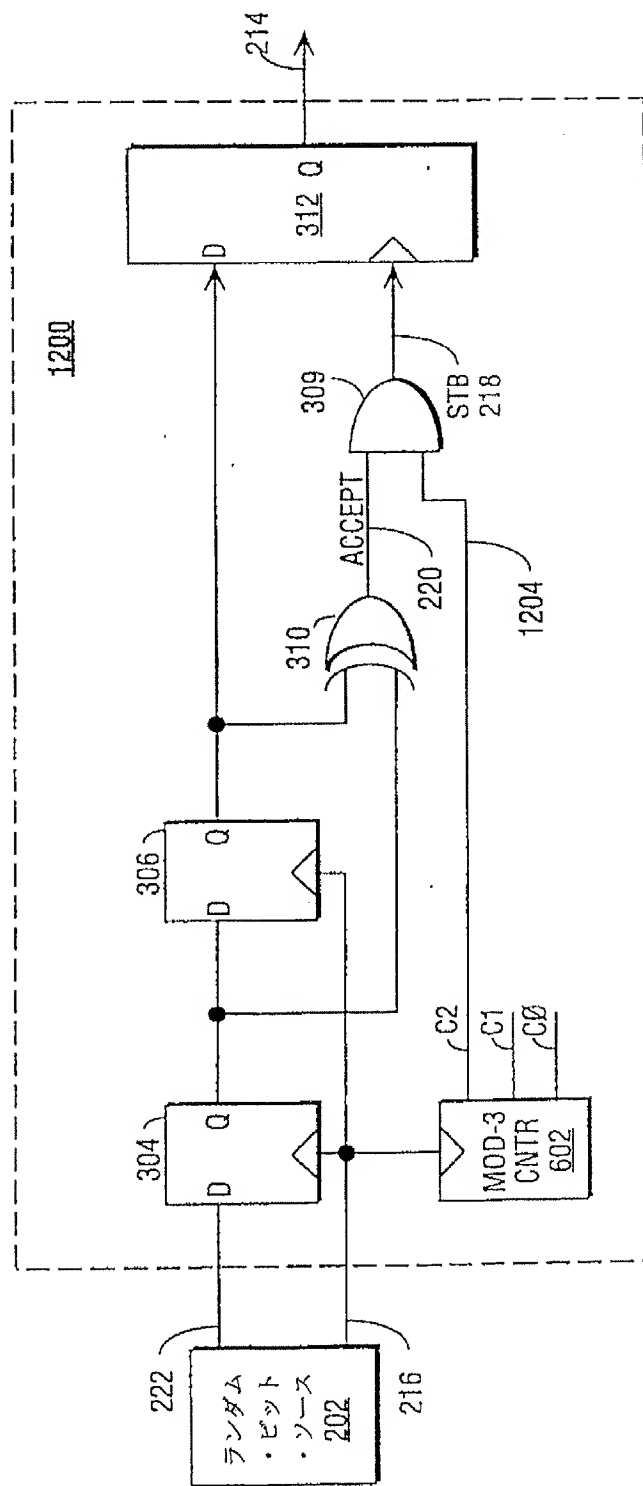
【図10】



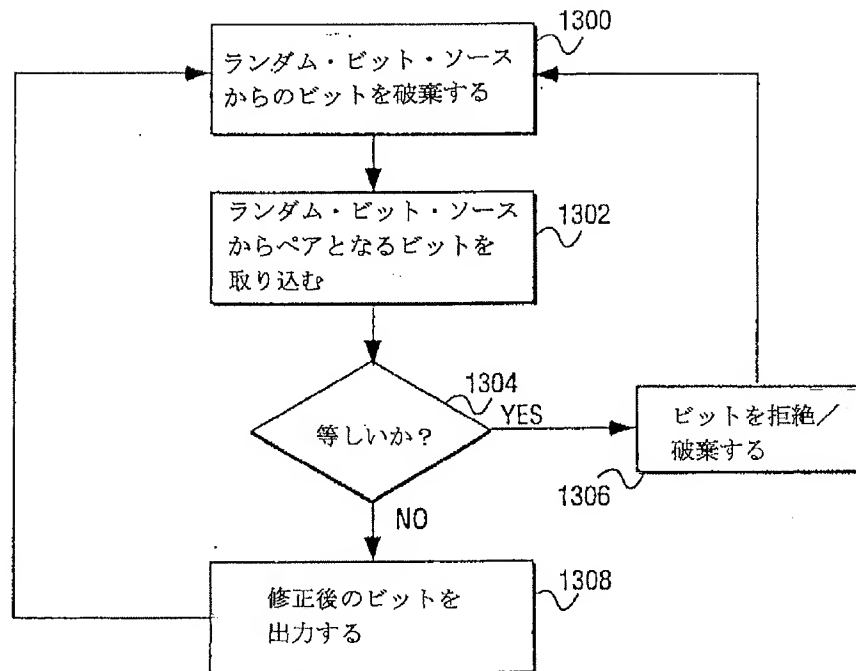
【図11】



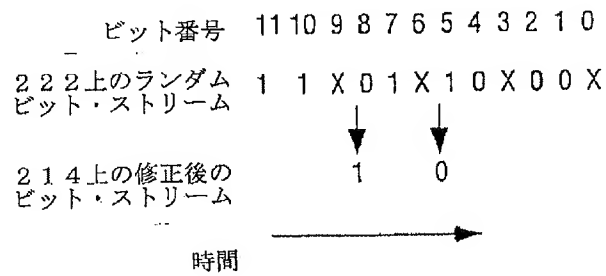
【図12】



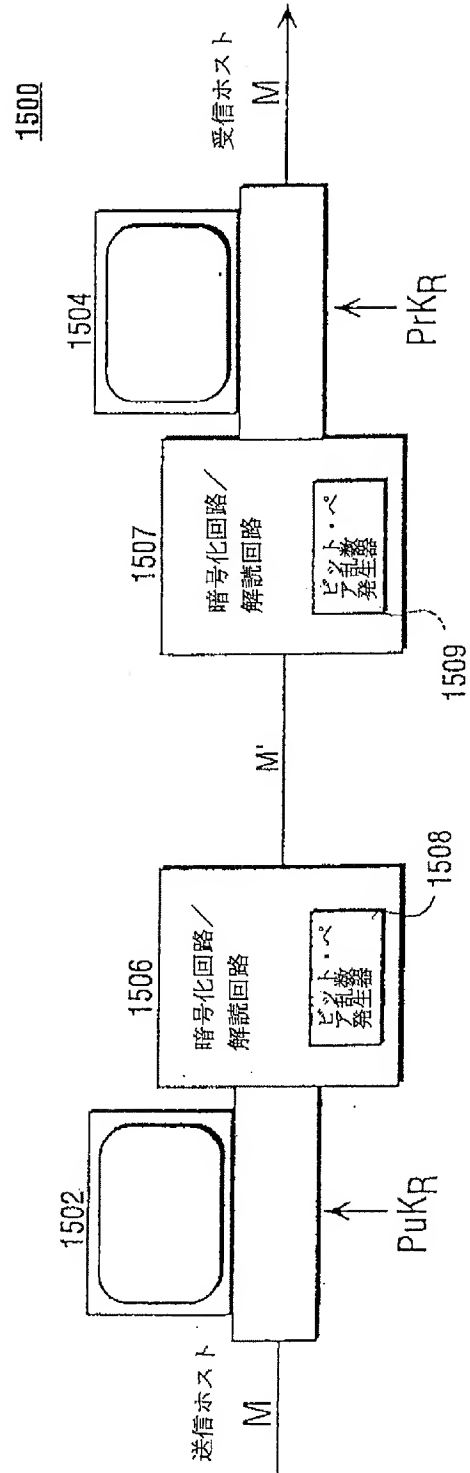
【図13】



【図14】



【図15】



INTERNATIONAL SEARCH REPORT

International Application No.
PCT/US 00/06916

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 H04L9/22

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 7 H04L

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

EPO-Internal, WPI Data, INSPEC

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	US 5 844 925 A (DENT PAUL W) 1 December 1998 (1998-12-01) abstract column 3, line 43 - column 4, line 32 column 5, line 12 - line 41 claim 1 figure 3	1,2,4-8, 10,17
A	DE 40 06 251 C (WOLFGANG BITZER) 11 April 1991 (1991-04-11) abstract column 1, line 3 - line 35 column 2, line 16 - line 50 figure 3	1,2,10
-/-		

☒ Further documents are listed in the continuation of box D.

☒ Patent family members are listed in annex.

* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubt on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, each combination being obvious to a person skilled in the art

"Z" document member of the same patent family

Date of the actual completion of the international search

15 September 2000

Date of mailing of the international search report

21/09/2000

Name and mailing address of the ISA
European Patent Office, P.B. 5018 Patentkan 2
NL - 2250 HV Rijswijk
Tel. (+31-70) 340-2040, Tx 31 651 epo.nl,
Fax: (+31-70) 340-3016

Authorized officer

Gautier, L

Form PCT/ISA/210 (second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

International Application No.
PCT/US 00/06916

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT		
Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	<p>US 5 781 458 A (GILLEY JAMES E) 14 July 1998 (1998-07-14) abstract column 2, line 63 -column 3, line 12 column 5, line 19 - line 43 figures 3,4</p>	1,10,17

1

Form PCT/ISA/210 (continuation of second sheet) (July 1992)

page 2 of 2

INTERNATIONAL SEARCH REPORT

Information on patent family members

International Application No.

PCT/US 00/06915

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 5844925 A	01-12-1998	AU 718539 B	13-04-2000
		AU 3959597 A	09-02-1998
		CA 2258362 A	22-01-1998
		CN 1225769 A	11-08-1999
		EP 0913040 A	06-05-1999
		WO 9802990 A	22-01-1998
DE 4006251 C	11-04-1991	NONE	
US 5781458 A	14-07-1998	NONE	

Form PCT77/BA210 (patent family search) (July 1982)

フロントページの続き

(81) 指定国 EP(AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OA(BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG), AP(GH, GM, KE, LS, MW, SD, SL, SZ, TZ, UG, ZW), EA(AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), AE, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CR, CU, CZ, DE, DK, DM, DZ, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, US, UZ, VN, YU, ZA, ZW